

Abstract

Malicious software attacks (such as for example stealing data, changing data or destroying data) on personal computers and/or servers and/or other computerized gadgets (especially through the Internet) are becoming more and more common and more and more dangerous, causing damages of tens of billions of dollars each year. The state-of-the-art solutions are inherently limited because they solve only a limited number of problems on the surface, instead of going deeply into the roots of the problem. The most common solutions are Anti-viruses and firewalls. Anti-viruses are limited because they can only detect known viruses or worms that have already been identified (usually after they have already attacked many computers). Network firewalls are typically based on packet filtering, which is limited in principle, since the rules of which packets to accept or not may contain for example subjective decisions based on trusting certain sites or certain applications. However, once security is breached for any reason, for example due to an error or intended deception, a hostile application may take over the computer or server or the entire network and create unlimited damages (directly or by opening the door to additional malicious applications). They are also not effective against security holes for example in browsers or e-mail programs or in the operating system itself. According to an article in ZDnet from Jan 24, 2001, security holes in critical applications are discovered so often that just keeping up with all the patches is impractical. Also, without proper generic protection for example against Trojan horses, which can identify any malicious program without prior knowledge about it, even VPNs (Virtual Private Networks) and other form of data encryption, including digital signatures, are not really safe because the info can be stolen before or below the encryption. Even personal firewalls are typically limited, because once a program is allowed to access the Internet, there are no other limitations for example on what files it may access and send or what it might do. The present invention creates a general generic comprehensive solution by going deeply into the roots of the problem. One of the biggest absurdities of the state-of-the-art situation is that by default programs are allowed to do whatever they like to other programs or to their data files or to critical files of the operating system, which is as absurd as letting a guest in a hotel bother any other guests as he pleases, steal their property or copy it or destroy it, destroy their rooms, etc., or for example have free access to the hotel's safe or electronic switchboard or phone or elevator control room. The present concept is based on automatic segregation between programs: It is like limiting each guest by default to his room and limiting by default his access to the Hotel's strategic resources, so that only by explicit permission each guest can get additional privileges.